

Re: Can the Shor oracle be used to prove that a function is constant?

Source: <http://sci.tech-archive.net/Archive/sci.physics.research/2004-08/0317.html>

From: Greg Kuperberg (greg_at_conifold.math.ucdavis.edu)

Date: 08/16/04

Date: 16 Aug 2004 13:56:02 -0400

davidedc <davidedc@yahoo.com> wrote in message news:<40eaf3b9\$1@news.sentex.net>...

- > Given a function $f: \{0,1\}^n \rightarrow \{0,1\}$, would it be possible to use the
- > Shor Oracle to figure out if f is constant?
- >
- > With this I mean: determine the period on the output qbit, obtained
- > applying a quantum implementation of f over the input qbits put in
- > superpositioned state. I guess that the period would be 1 iff the
- > function is constant?

As Peter Shor pointed out, Shor's algorithm works with statistical approximations. In other words it will find some p such that $f(x) = f(x+p)$ holds either always or at least usually. This is no help for the hard case of your question.

- > If this was feasible, then $P=NP$ because the SAT problem could be
- > addressed in polynomial time by performing a binary search on the
- > input space.

First, the correct statement is that if there is a quantum polynomial time algorithm to determine if an arbitrary f is constant, then BQP contains NP. BQP, not P, is the complexity class for quantum polynomial time. Unlike P, BQP it is not a priori a subset of NP.

Second, the best algorithm for your question is the Grover search, which can find a solution to $f(x) = 1$ in time $O(\sqrt{2^n})$. This is a surprising result, because a classical blind search of course takes linear time. But $O(\sqrt{2^n})$ is not polynomial time. Moreover, if you sequester f in a black box, then it is a theorem that Grover's algorithm is optimal.

Indeed, one way to state the P vs NP problem is by asking: How much do you lose by sequestering the function f in a black box? If $P = NP$, then you could miraculously solve the equation $f(x) = 1$ in polynomial time, for any f computable in polynomial time, in effect by analyzing the

sci.physics.research: Re: Can the Shor oracle be used to prove that a function is constant?

algorithm to compute f.

```
--  
  /\ Greg Kuperberg (UC Davis)  
 /  \  
\  / Visit the Math ArXiv Front at http://front.math.ucdavis.edu/  
\  / * All the math that's fit to e-print *
```